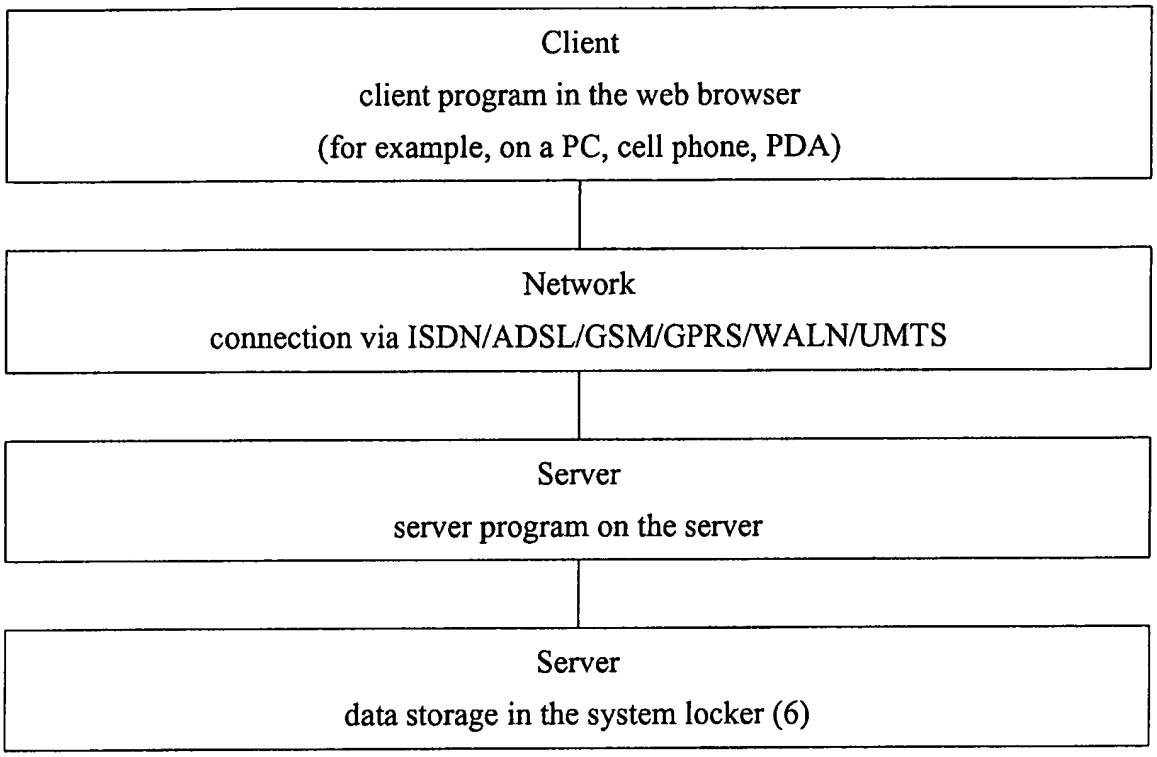
Client
client program in the web browser
(for example, on a PC, cell phone, PDA)
Network
connection via ISDN/ADSL/GSM/GPRS/WALN/UMTS
Server
server program on the server
Server
data storage in the system locker (6)

Fig. 1

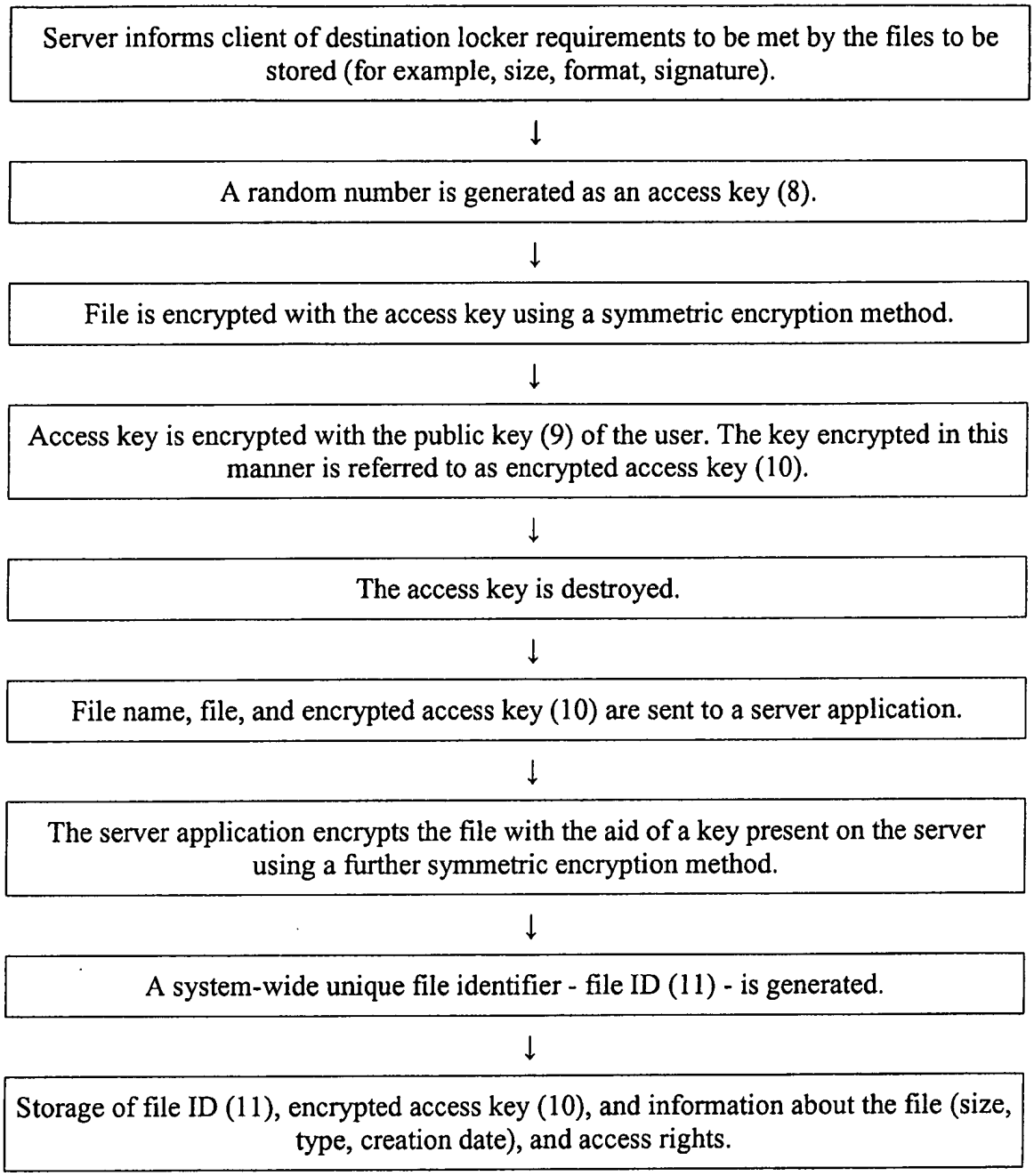
Server informs client of destination locker requirements to be met by the files to be stored (for example, size, format, signature).
A random number is generated as an access key (8).
File is encrypted with the access key using a symmetric encryption method.
Access key is encrypted with the public key (9) of the user. The key encrypted in this manner is referred to as encrypted access key (10).
The access key is destroyed.
File name, file, and encrypted access key (10) are sent to a server application.
The server application encrypts the file with the aid of a key present on the server using a further symmetric encryption method.
A system-wide unique file identifier - file ID (11) - is generated.
Storage of file ID (11), encrypted access key (10), and information about the file (size, type, creation date), and access rights.

Fig. 2

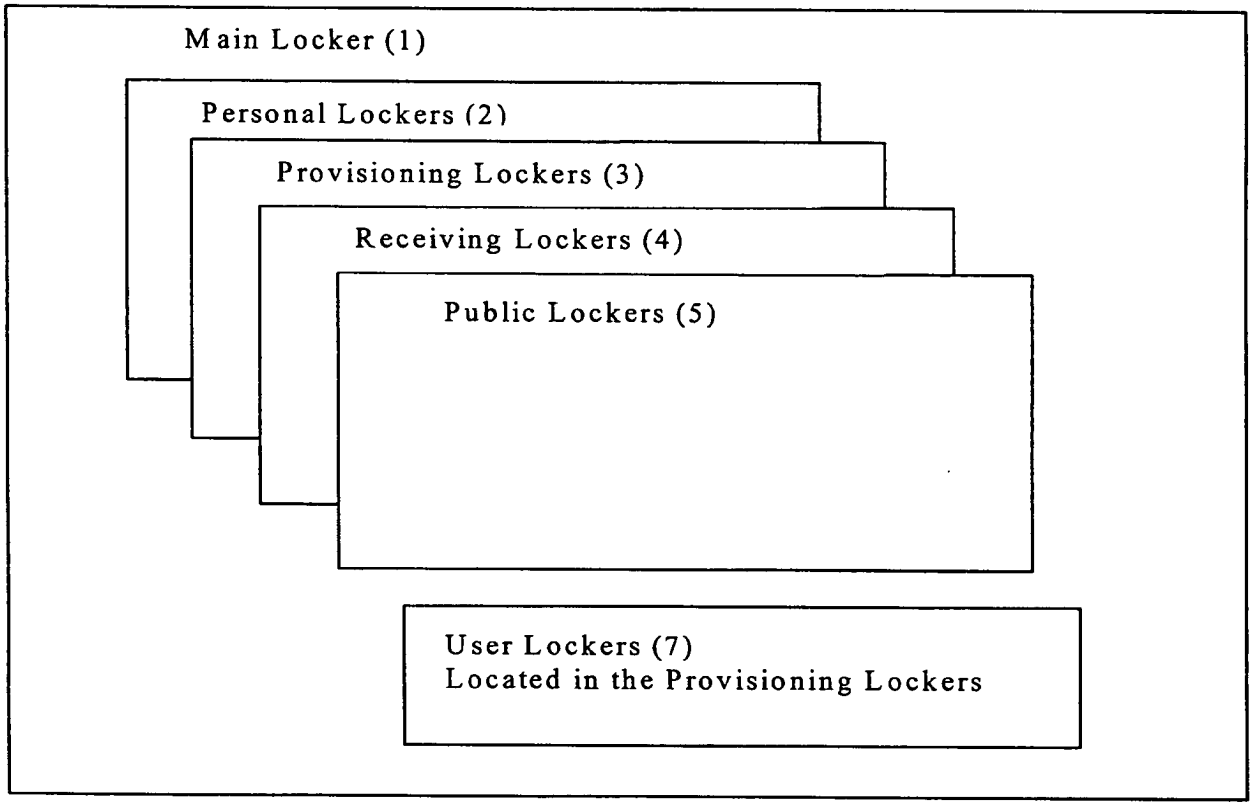
Main Locker (1)
Personal Lockers (2)
Provisioning Lockers (3)
Receiving Lockers (4)
Public Lockers (5)
User Lockers (7)
Located in the Provisioning Lockers

Fig. 3